

REMARKS

Status of claims

Prior to the present Amendment, claims 29 – 53, 57 and 58 were pending, of which 29, 57 and 58 are independent.

Now claims 30, 32 – 37, 41, 48, and 51 – 53 are being canceled.

Claims 29, 57 and 58 are amended.

New claims 59 and 60 – 67 are presented.

Both independent claims 29 and 59, as well as independent amended claims 57 and 58, are further defined and amended by the new expressions:

- "with application-specific or system-specific initialization data (DI, A-I, I-I)"
- and "to put into operation (new data carriers), new applications or extension of applications".

This is described in the original application (as published as US 2003/0033527 A1) in paragraphs [0002], [0005], [0008], [0009] and further in paragraphs [0038], [0039], [0062], [0063] and also in original claims 10, 11, 12.

To more clearly distinguish the present invention from all cited references and prior art, independent claims 29, 57 and 58 have been amended. Furthermore, new independent claim 59 -- and claims 60 – 67 which correspond to previous claims 31, 32, 42, 43, 45, 47, 49, 50 but are depending on new claim 59 -- are presented.

The claimed invention

Some features of the claimed invention are:

This initialization comprises application-specific or system-specific initialization data (DI, A-I, I-I) and with this initialization and initialization data from a remote authorization authority (HA), at a decentralized read and write station, the read and write station (WRk) (claim 59) or mobile data carriers (IMj) (claim 29) are initialized to put in into operation new data carriers, new applications or extension of applications.

The initialization process is extensively explained in the examples and for the figures of the description.

Cited References

The cited references Eberhard (5,473,689) and Sciupac (US 6,871,278) do not disclose such an initialization process with such initialization data and especially not the methods for the initialization of decentralized read and write stations (WR) and of data carriers (IM) at a decentralized authorized read and write station with these initialization data from a remote authorization authority (HA).

The goals of these references are entirely different as compared to the goals of the present invention.

Reference Eberhard discloses a new method for mutual authentication between a first electronic device (a read and write station) and a second electronic device (a mobile data carrier) for communication with improved security. This method is including an encryption with two random numbers generated in the first electronic device.

Reference Sciupac discloses a transaction system for secure communication and authentication between a read and write station 10 and a data carrier 12 and a host computer 14. The read and write station stores cryptographic keys and firmware for executing the secure protocols.

In principle these cited references only deal with a first step: the authentication and establishing of a secure communication and not with a second step of initialization according to claims 29 and 59.

In the present claimed invention, in contrast, after such a first step of authentication and establishing of a secure communication between the four elements:

- authorization medium (AM),
- authorization authority (HA),

- read and write stations (A-WR, WR) and
- data carrier (IM)

in a second step the inventive initialization is carried out in the secured communication.

Claim Rejections – 35 USC 102

The independent claims 29, 57 and 58 were rejected as being anticipated by reference Eberhard (US 5,473,689). The Examiner cites column 3, lines 3 to 36 and 45 – 67 and column 4, lines 1 – 9 against the content of previous claim 29.

But the undersigned has diligently reviewed the cited portions of Eberhard and is unable to see a method of initialization according to the new claims 29 and 59. Nor is the undersigned able to find such a limitation anywhere in Eberhard.

E.g. the random numbers Z1, Z2 of Fig. 2 in Eberhard are not application-specific with respect to the system-specific initialization data (DI, A-I, I-I). They only serve for the encryption in the mutual authentication of the two electronic devices:

1. read and write station
2. mobile data carrier

These random numbers cannot contain any message.

Further: The inventive methods include the four system elements:

1. read and write station (WR, A-WR)
2. data carrier (IM)
3. remote authorization authority (HA)
4. authorization means (AM).

Eberhard deals only with a 1. element = first electronic device (WR) and a 2. element = second electronic device (IM), meaning that there is no third and no forth element.

The cited references of Eberhard and Sciupac as well as the further cited prior art do not disclose the new and inventive method for initialization according to the features and limitations of present independent claims 29, 57, 58 and 59.

Also from a combination of these references there is no indication for these new features of the present

invention.

Therefore the independent claims 29, 57, 58 and 59 should be allowable and with them also the depending claims.

Reconsideration is requested.

Respectfully submitted,

/s/

Carl Oppedahl
PTO Reg. No. 32746